**Final Project Report**

On

**Implementation of Dynamic Routing on a campus network**

Submitted in partial fulfillment of the requirements for the award of degree of

**BACHELOR OF ENGINEERING**

**IN**

**COMPUTER SCIENCE & ENGINEERING**



**Submitted By: Project mentor: Er. Indejeet Singh**

**Simranjeet Singh**

**17BCS1708**

**Signature and Remarks of mentor**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**CHANDIGARH UNIVERSITY, GHARUAN**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

### CERTIFICATE

This is to certify that the work embodied in this Project Report entitled **“Implementation of Dynamic Routing on a campus network ”** being submitted by **Simranjeet Singh,UID-17BCS1708,** 6th Semester for partial fulfillment of the requirement for the degree of **“ Bachelor of Engineering in Computer Science & Engineering ”** discipline in “ **Chandigarh University** ” during the academic session JAN-MAY 2020 is a record of bonafide piece of work, carried out by student under my supervision and guidance in the **“ Department of Computer Science & Engineering ”, Chandigarh University.**

**APPROVED & GUIDED BY: ER. Inderjeet Singh**

**ACKNOWLEGMENT**

While presenting this report we would like to express my deep sense of gratitude to AP. Navpreet Kaur that was indispensable part of my project giving me unending guidance, inspiration, encouragement and providing me excellent environment throughout my project training at Chandigarh University. The training was an extremely productive & enriching experience, not only technically but also from providing practical skills.

We are extremely thankful to AP. Navpreet Kaur who had devoted a lot of time in guiding and supervising me during my project training. We place our gratitude towards our mentor for her valuable advice and guidance in carrying out this enjoyable and productive experience, which provided me a great opportunity to search new horizons.

Contents

[**Implementation of Dynamic Routing on a campus network** 1](#_Toc37603585)

[CERTIFICATE 2](#_Toc37603586)

[Chapter 1- Introduction 7](#_Toc37603587)

[1.1 Network 7](#_Toc37603588)

[**1.2 Network Security** 8](#_Toc37603589)

[**Chapter 2- Requirements** 10](#_Toc37603590)

[2.1 Hardware Requirements 10](#_Toc37603591)

[2.2 Software Requirements 11](#_Toc37603592)

[2.3 Network Designing: 13](#_Toc37603593)

[Chapter 3- Architecture Diagram 15](#_Toc37603594)

[Chapter 4- Project Methodology 16](#_Toc37603595)

[4.1 Interface 16](#_Toc37603596)

[**4.2 Module Description** 16](#_Toc37603597)

[4.2.1 Server: 16](#_Toc37603598)

[**4.2.2 Domain Name System:** 17](#_Toc37603599)

[4.2.3 Dynamic Host Control Protocol: 17](#_Toc37603600)

[4.2.4 Network switch: 17](#_Toc37603601)

[**Chapter 5- Project Implementation** 19](#_Toc37603602)

[5.1 Routing Protocol 19](#_Toc37603603)

[**5.1.1 EIGRP (Enhanced Interior Gateway Routing Protocol):** 19](#_Toc37603604)

[**5.1.2 OSPF(Open Shortest Path First) :** 20](#_Toc37603605)

[**5.1.3 Static routing:** 21](#_Toc37603606)

[5.2 DNS (Domain Name System/Server): 22](#_Toc37603607)

[5.3 SMTP (Simple Mail Transfer Protocol): 22](#_Toc37603608)

[5.4 Access-List: 24](#_Toc37603609)

[5.5 NAT (Network Address Translation): 26](#_Toc37603610)

[Chapter 6- Results 27](#_Toc37603611)

[6.1 Screenshots 27](#_Toc37603612)

[6.2 Output validation and Comparison: 31](#_Toc37603613)

[Chapter 7- Conclusion and Future scope 32](#_Toc37603614)

[Chapter 8- References 33](#_Toc37603615)

LIST OF FIGURES

[Figure 1Cisco Packet Tracer Lab 11](#_Toc23942302)

[Figure 2 : Overall design 13](#_Toc23942303)

[Figure 3:show the circuit and connection are completed 14](#_Toc23942304)

[Figure 4: different servers and routers 14](#_Toc23942305)

[Figure 5:overall design 27](#_Toc23942306)

[Figure 6: show the circuit and connection are completed 27](#_Toc23942307)

[Figure 7:Different servers and routers 28](#_Toc23942308)

[Figure 8:Main router- other block are connected with it. 28](#_Toc23942309)

[Figure 9:Username and password are added in database of Gmail 29](#_Toc23942310)

[Figure 10:E-mail is received by user1 and we can reply back to him by click on reply button 29](#_Toc23942311)

[Figure 11:Service of file transfer protocol (FTP) is used 30](#_Toc23942312)

[Figure 12:Protocol ftp is used and text is create and read by the user 30](#_Toc23942313)

[Figure 13:DHCP protocol 31](#_Toc23942314)

Abstract

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them (Navpreet, 2014).

So it is very important for all the users to get familiar with various aspects of Network Security. In the article basics of Network Security are discussed. With the millions of Internet users able to pass information from the network, the security of business networks is a major concern. The very nature of the Internet makes it vulnerable to attack. The hackers and virus writers try to attack the Internet and computers connected to the Internet. With the growth in business use of the Internet, network security is rapidly becoming crucial to the development of the Internet. Many business set up firewalls to control access to their networks by persons using the Internet.

# Chapter 1- Introduction

## 1.1 Network

* It is the interconnection of multiple devices, generally termed as Hosts connected using multiple paths for the purpose of sending/receiving data or media. There are also multiple devices or mediums which helps in the communication between two different devices which are known as **Network devices**. Ex: Router, Switch, Hub, Bridge.  
  The layout pattern using which devices are interconnected is called as network topology. Such as Bus, Star, Mesh, Ring, Daisy chain.
* **OSI:** OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
* **Protocol:** A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.

1. **Routing Information Protocol (RIP)** is a distance vector protocol that uses [hop count](https://whatis.techtarget.com/definition/hop) as its primary metric. RIP defines how [routers](https://searchnetworking.techtarget.com/definition/router) should share information when moving traffic among an interconnected group of local area networks ([LANs](https://searchnetworking.techtarget.com/definition/local-area-network-LAN)). RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination. Each RIP router maintains a [routing table](https://searchnetworking.techtarget.com/definition/routing-table), which is a list of all the destinations the router knows how to reach.
2. **Open Shortest Path First (OSPF)** is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP) i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).
3. [**Enhanced Interior Gateway Routing Protocol (EIGRP)**](https://www.geeksforgeeks.org/computer-network-features-enhanced-interior-gateway-routing-protocol-eigrp/) is a dynamic routing Protocol which is used to find the best path between any two layers 3 device to deliver the packet. EIGRP works on network layer Protocol of osi model and uses the protocol number 88

**We are using the RIP protocol to connect the different with each other.**

**1.2 Network Security**

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

Network security ensures the factor for a new system with higher-level security standards for the information exchange. Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

In order to minimize susceptibility to malicious attacks from external threats to the network, corporations often employ tools which carry out network security verifications.

**Access-list:** Access Control List (ACL) are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for the network. This can be applied to routers (Cisco).ACLs provide a powerful way to control traffic into and out of your network; this control can be as simple as permitting or denying network hosts or addresses.  You can configure ACLs for all routed network protocols. The most important reason to configure ACLs is to provide security for your network. However, ACLs can also be configured to control network traffic based on the TCP port being used.

**NAT (Network Address Translation):** Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

**DES (Data Encryption Standard**): DES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

**AES (Advanced Encryption Standard):** It is found at least six times faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

**Chapter 2- Requirements**

To complete the work on network security, I take help from some software requirements. Software requirements as

* Operating System : Windows7 ultimate upto upgrades versions
* Front end tools : Cisco Packet Tracer version 6.0.1, GNS 3

**Windows 7** is a personal computer [operating system](http://en.wikipedia.org/wiki/Operating_system) developed by [Microsoft](http://en.wikipedia.org/wiki/Microsoft), a version of [Windows NT](http://en.wikipedia.org/wiki/Windows_NT). Development of 7 occurred as early as 2006 under the codename "Blackcomb". Windows 7 was released to manufacturing on July 22, 2009, and became generally available on October 22, 2009, less than three years after the release of its predecessor, [Windows Vista](http://en.wikipedia.org/wiki/Windows_Vista).  While retaining a similar appearance to Vista, 7's [interface](http://en.wikipedia.org/wiki/Windows_Aero) was streamlined, with the addition of a redesigned [taskbar](http://en.wikipedia.org/wiki/Taskbar) that allows applications to be "pinned" to it, and new window management features. Other new features were added to the operating system, including libraries, the new file sharing system HomeGroup, and support for [multitouch](http://en.wikipedia.org/wiki/Multitouch) input.

## 2.1 Hardware Requirements

Table Minimum hardware requirements for Windows 7

|  |  |  |
| --- | --- | --- |
|  | | |
| Component | Operating system architecture | |
| 32-bit | 64-bit |
| [Processor](http://en.wikipedia.org/wiki/Central_processing_unit) | 1 GHz [IA-32](http://en.wikipedia.org/wiki/IA-32) processor | 1 GHz [x86-64](http://en.wikipedia.org/wiki/X86-64) processor |
| [Memory (RAM)](http://en.wikipedia.org/wiki/Random_Access_Memory) | 1 GB | 2 GB |
| [Graphics card](http://en.wikipedia.org/wiki/Graphics_card) | [DirectX 9](http://en.wikipedia.org/wiki/DirectX_9) graphics processor with [WDDM](http://en.wikipedia.org/wiki/Windows_Display_Driver_Model) driver model 1.0 (Not absolutely necessary; only required for [Aero](http://en.wikipedia.org/wiki/Windows_Aero)) | |
| Free [hard drive](http://en.wikipedia.org/wiki/Hard_Disk_Drive) space | 16 GB | 20 GB |
| [Optical drive](http://en.wikipedia.org/wiki/Optical_drive) | DVD-ROM drive (Only to install from DVD-ROM media) | |

**Hardware Used**

* Routers : Cisco 2811 Series.
* Switches : Cisco 2960 Series.
* Devices : Computers, Servers, Wireless Routers.
* Other Media : Console cables, Ethernet cables, Serial cable etc.

## 2.2 Software Requirements

**Cisco Packet Tracer** Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

**Purpose:** The purpose of this lab is to become familiar with the Packet Tracer interface.

**Software Used**

* Operating System **:** Windows 2012 SERVER, Windows7 etc.
* Front end tools **:** Cisco Packet Tracer.

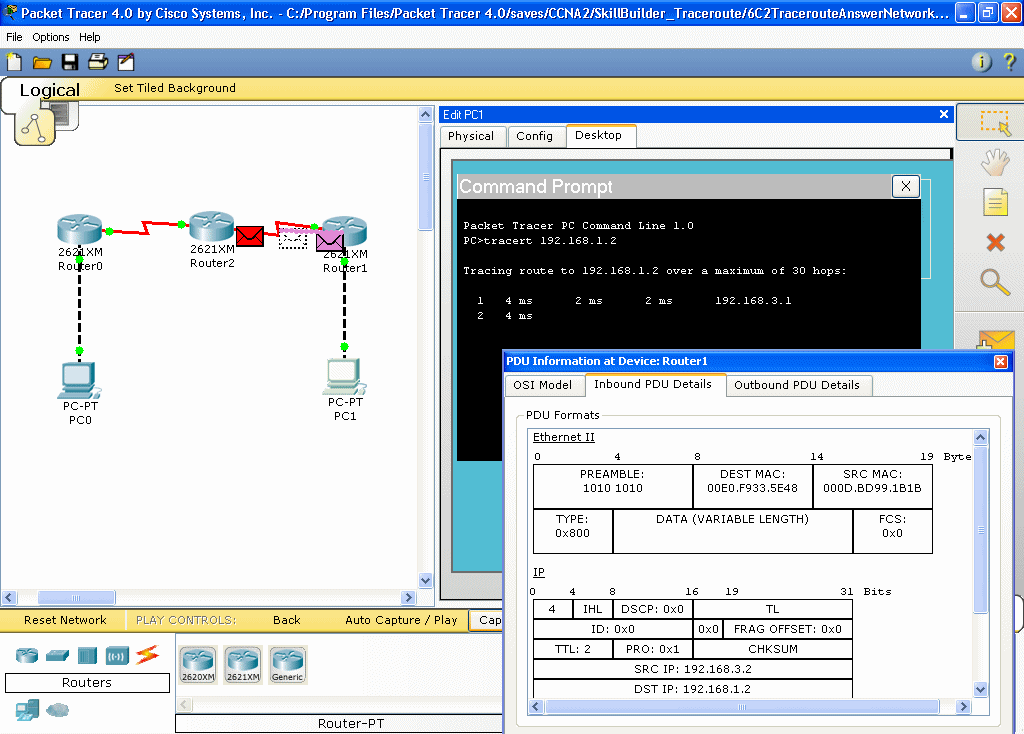
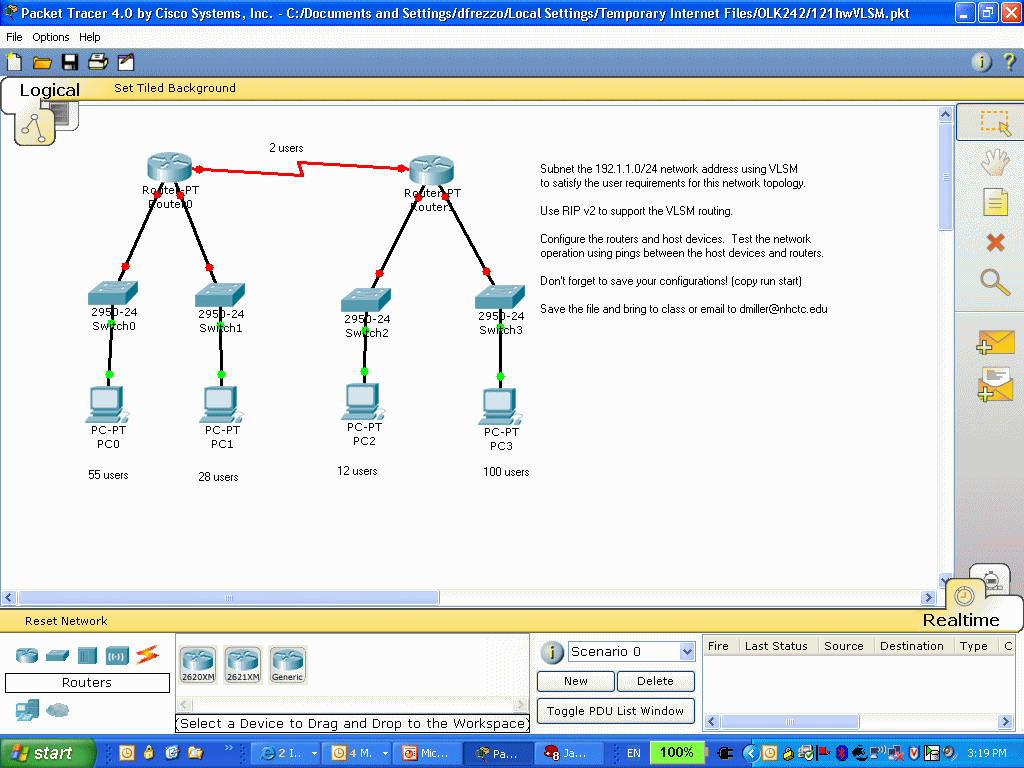


Figure Cisco Packet Tracer Lab

## 2.3 Network Designing:

There are 4 blocks which are interconnected with each other. Some of the blocks use the network security in which some of the websites and unauthorized sites are blocked.

**List of Figures of Network routing of OSPF & EIGRP with different autonomous system**

1. Internet topologies
2. Configuration view of internet topologies
3. Routing OSPF with different autonomous system
4. IP configuration
5. Routing EIGRP with different autonomous system
6. Redistribution of EIGRP 10 & 20
7. Redistribution of OSPF & EIGRP
8. Web server
9. DNS server
10. Exchange server
11. Access list security
12. Standard access list security

Ex-standard access list security

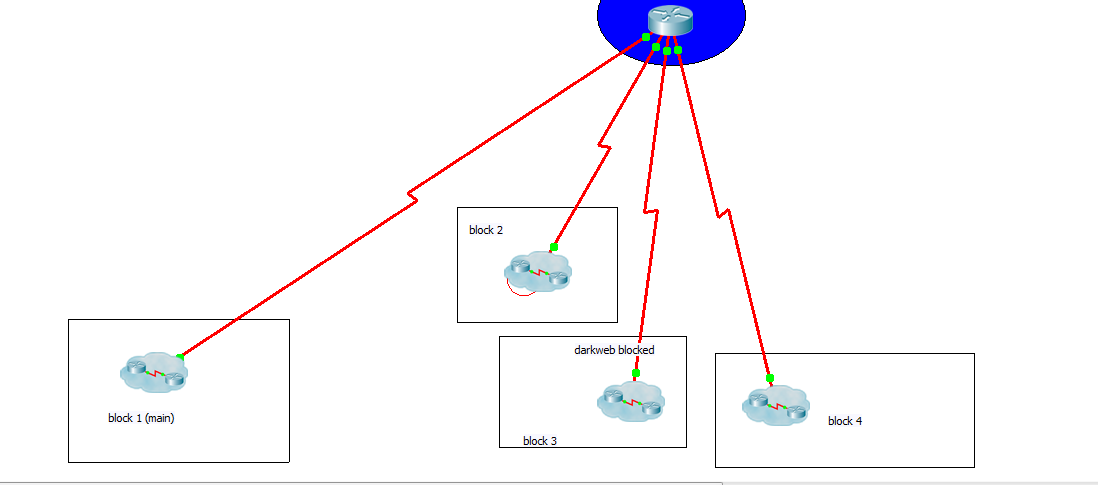
****

Figure : Overall design

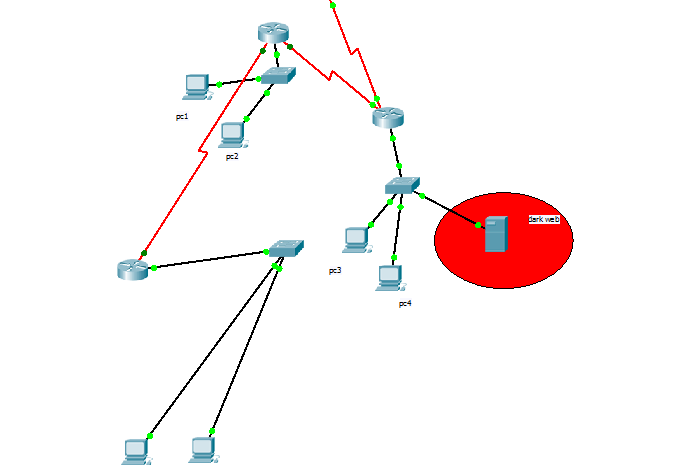


Figure :show the circuit and connection are completed

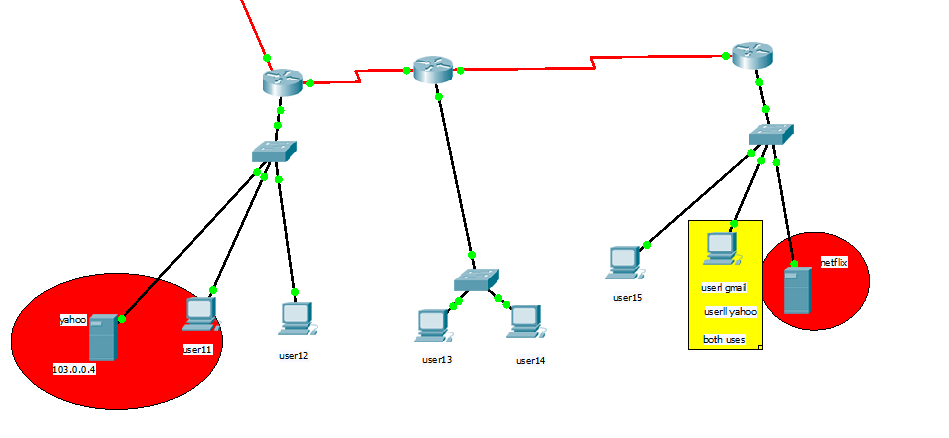


Figure : different servers and routers

# Chapter 3- Architecture Diagram

**Access applied**

**DHCP protocol**

**Delivered**

**Two Way Authentications**

**Messaging protocol**

We can communicate with different clients at any time and can send the messages. During the communication, the data has to transmit securely.

There are different routers which are connected through the switches and the different clients are connected with it and the different ip address is allocated for the security.

# Chapter 4- Project Methodology

## 4.1 Interface

A server is a system ([software](http://en.wikipedia.org/wiki/Computer_software) and suitable [computer hardware](http://en.wikipedia.org/wiki/Computer_hardware)) that responds to requests across a [computer network](http://en.wikipedia.org/wiki/Computer_network) to provide, or help to provide, a [network service](http://en.wikipedia.org/wiki/Network_service). Servers can be run on a dedicated computer, which is also often referred to as "the server", but many networked computers are capable of hosting servers. In many cases, a computer can provide several services and have several servers running. Many servers do not have a [graphical user interface](http://en.wikipedia.org/wiki/Graphical_user_interface) (GUI) as it is unnecessary and consumes resources that could be allocated elsewhere. Similarly, audio and [USB](http://en.wikipedia.org/wiki/Universal_Serial_Bus) interfaces may be omitted. With the help of GUI (Graphic User Interface), server works and perform multitasks.

**4.2 Module Description**

### 4.2.1 Server:

A server is a computer program that provides services to other computer program (and their users), in the same or other computer. The physical computer that runs a server program is also often referred to as server. Services can be supplied centrally by the use of a server; in other cases all the machines on a network have the same status with no dedicated server, and services are supplied peer -to- peer.

Server used as an adjective, as in server operating system, refers to the product’s ability to handle multiple requests, and is said to be “ server- grade”. A server operating system is intended or better enabled to run server applications. The differences between the server and workstation versions of a product can vary from the removal of an arbitrary software limits due to licensing, as in the case of window 2000, or the addition of bundled applications as in Mac OS X Server.

A server can also refer to a computer that has been set aside to run a specific server application. Server application can be divided among server computers over an extreme range, depending upon the workload. A web server application (such as the [multi platform](http://en.wikipedia.org/wiki/Multiplatform) "[Apache HTTP Server](http://en.wikipedia.org/wiki/Apache_HTTP_Server)". This web server software can be run on any capable [computer](http://en.wikipedia.org/wiki/Computer). For example, while a [laptop](http://en.wikipedia.org/wiki/Laptop) or personal computer is not typically known as a server, they can in these situations fulfill the role of one, and hence be labeled as one. It is, in this case, the machine's role that places it in the category of server.

**4.2.2 Domain Name System:**

**DNS** is a [hierarchical](http://en.wikipedia.org/wiki/Hierarchical) distributed naming system for computers, services, or any resource connected to the [Internet](http://en.wikipedia.org/wiki/Internet) or a [private network](http://en.wikipedia.org/wiki/Private_network). It associates various information with [domain names](http://en.wikipedia.org/wiki/Domain_name) assigned to each of the participating entities. Most prominently, it translates easily memorized [domain names](http://en.wikipedia.org/wiki/Domain_name) to the numerical [IP addresses](http://en.wikipedia.org/wiki/IP_address) needed for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the [Internet](http://en.wikipedia.org/wiki/Internet).

An often-used analogy to explain the Domain Name System is that it serves as the [phone book](http://en.wikipedia.org/wiki/Telephone_directory) for the Internet by translating human-friendly computer [hostnames](http://en.wikipedia.org/wiki/Hostname) into IP addresses.

### 4.2.3 Dynamic Host Control Protocol:

**DHCP** is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts. The most essential information needed is an IP address, and a default route and routing prefix. DHCP eliminates the manual task by a network administrator. It also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.

In addition to IP addresses, DHCP also provides other configuration information, particularly the IP addresses of local caching DNS resolvers, network boot servers, or other service hosts.

### 4.2.4 Network switch:

Switch is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the Data Link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as layer 3 switches or multilayer switches.

The term network switch does not generally encompass unintelligent or passive network devices such as hubs and repeaters.

**Functions:**

* Learning
* Forward and filtering
* Loop Avoidance



**Chapter 5- Project Implementation**

## 5.1 Routing Protocol

**5.1.1 EIGRP (Enhanced Interior Gateway Routing Protocol):**

Advanced version of IGRP developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.

**Features:** -

* Cisco proprietary
* Hybrid protocol
  + Link State
  + Distance Vector
* Multicast Updates using
* Address 224.0.0.10
* Support VLSM
* Automatic Route Summarization
* Unequal path cost load balancing
* Metric (32 bit composite)
  + Bandwidth
  + Delay
  + Load
  + Reliability
  + MTU
* Neighbor Recovery
* Triggered updates
* Backup Route
* **Configuring EIGRP**

Router (config) #router eigrp<as no>

Router (config-router) #network <net addr.>

Router (config-router) #network <net addr.>

Router (config-router) #exit

**5.1.2 OSPF (Open Shortest Path First) :**

Link-state, hierarchical IGP routing protocol proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the ISIS protocol.

#### Commands to configure OSPF

Router#conf t

Router (config) #router ospf<process no>

Router (config-router) #network <net address><wild mask> area <area id>

Router (config-router) #network <net address><wild mask> area <area id>

Router (config-router) #exit

**Using commands:**

1. interface FastEthernet0/0
2. ip address 50.0.0.1 255.0.0.0
3. ip access-group hcl in
4. ip access-group 10 out
5. ip nat inside
6. duplex auto
7. speed auto
8. !
9. interface FastEthernet0/1
10. no ip address
11. duplex auto
12. speed auto
13. shutdown
14. !
15. interface Serial0/0/0
16. ip address 40.0.0.2 255.0.0.0
17. clock rate 2000000
18. !
19. interface Serial0/0/1
20. no ip address
21. clock rate 2000000
22. shutdown
23. !
24. interface Vlan1
25. no ip address
26. shutdown
27. !
28. router rip
29. version 1
30. network 40.0.0.0
31. !
32. ip nat inside source static 50.0.0.2 30.0.0.3
33. ip nat inside source static 50.0.0.3 30.0.0.4
34. ip nat inside source static 50.0.0.4 30.0.0.5
35. ip nat inside source static 50.0.0.2 40.0.0.3
36. ip nat inside source static 50.0.0.3 40.0.0.4
37. ip nat inside source static 50.0.0.4 40.0.0.5
38. ip classless
39. ip route 10.0.0.0 255.0.0.0 40.0.0.1
40. ip route 20.0.0.0 255.0.0.0 40.0.0.1
41. ip route 30.0.0.0 255.0.0.0 40.0.0.1
42. !
43. ip flow-export version 9
44. !
45. !
46. access-list 10 deny 10.0.0.0 0.255.255.255
47. access-list 10 permit any
48. ip access-list extended hcl
49. deny tcp host 50.0.0.2 host 30.0.0.4 eq www
50. permit ip any any
51. !
52. !
53. !
54. !
55. !
56. line con 0
57. !
58. line aux 0
59. !
60. line vty 0 4
61. login
62. !
63. !
64. !
65. End

**5.1.3 Static routing:**

Static Routing is a form of routing that occurs when a router uses a manually configured routing entry, rather than information from a dynamic routing traffic.

**Configure terminal**

**ip route**{ ip-prefix | ip-addr/ip-mask } {[ next-hop | nh-prefix ] | [ interface next-hop | nh-prefix ]} [**name** nexthop-name] [**tag** tag-value] [ pref ]

or

**ipv6 route** ip6-prefix { nh-prefix | link-local-nh-prefix } | { nh-prefix [ interface ] | link-local-nh-prefix [ interface ]} [**name** nexthop-name] [**tag** tag-value] [ pref ]

(Optional) **show**{**ip** | **ipv6** }**static-route**

(Optional) **copy running-config startup-config**

## 5.2 DNS (Domain Name System/Server):

The most basic task of DNS is to translate hostnames to IP addresses. In very simple terms, it can be compared to a phone book. DNS also has other important uses.

Above all, DNS makes it possible to assign Internet names to organizations (or concerns they represent) independent of the physical routing hierarchy represented by the numerical IP address.

Because of this, hyperlinks and Internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form (such as "example.com"), which is easier to remember than the IP address 208.77.188.166. People take advantage of this when they recite meaningful URLs and e-mail addresses without caring how the machine will actually locate them.

The Domain Name System distributes the responsibility for assigning domain names and mapping them to IP networks by allowing an authoritative name server for each domain to keep track of its own changes, avoiding the need for a central register to be continually consulted and updated.

## 5.3 SMTP (Simple Mail Transfer Protocol):

**This protocol is used to send the E-mail to the other system and helps in communication. This protocol disturbs the outgoing mails only. Function of this protocol is to send the e-mail to other system.**

Step 1. In the CCM component, backup the /usr/local/tomcat/webapps/ROOT/WEB-INF/mail.properties file.

cp mail.properties mail.properties original

Step 2. Open the mail properties with a text editor and perform these changes:

vi mail.properties

# The hostname or IP address of your SMTP server

# Currently mob-gen.com email domain is hosted by gmail

# Gmail requires smtp over ssl, do not modify these settings

 Step 3. Use the IP address or Domain Name Server (DNS) for your SMTP server:

mail.smtp.host=<IP address or DNS>

Step 4. Use false for no authentication (With no authentication, anyone can use your SMTP server to send emails).

mail.smtp.auth=false

Step 5. Use port 25:

mail.smtp.port=25

mail.smtp.socketFactory.port=25

Step 6. Use com.sun.mail.smtp for SMTP on port 25:

mail.smtp.socketFactory.class=com.sun.mail.smtp

Step 7. Use true statement:

mail.smtp.socketFactory.fallback=true

Step 8. No changes:

# Email user to authenticate to gmail

mail.user.number=1

mail.user.1=

mail.password.1=

Step 9. The email that is used in order to send the email notification:

from.mail.user.1=<username@example.com>

Step 10. The username that is used:

from.mail.username.1=<username>

Step 11. Save the emailproperties file, it must look like this:

# The hostname or IP address of your SMTP server

# Currently mob-gen.com email domain is hosted by gmail

# Gmail requires smtp over ssl, do not modify these settings

mail.smtp.host=smtp.cloudcenter.com

mail.smtp.auth=false

mail.smtp.port=25

mail.smtp.socketFactory.port=25

mail.smtp.socketFactory.class=com.sun.mail.smtp

mail.smtp.socketFactory.fallback=true

# Email user to authenticate to gmail

mail.user.number=1

mail.user.1=

mail.password.1=

from.mail.user.1=noreply@cloudcenter.com

from.mail.username.1=CloudCenter Admin

## **5.4 Access-List:**

* Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistent access list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit deny statement that follows could cause immediate access problems.
* Another reason to configure an access list before applying it is because an interface with an empty access list applied to it permits all traffic.
* All access lists need at least one permit statement; otherwise, all packets are denied and no traffic passes.
* Organize your access list so that more specific references in a network or subnet appear before more general ones.
* A packet will match the first ACE in the ACL. Thus, a permit ip any any will match all packets, ignoring all subsequent ACES.
* Although all access lists end with an implicit deny statement, we recommend use of an explicit deny statement (for example, deny ip any any). On most platforms, you can display the count of packets denied by issuing the show access-list command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit deny statements are counted, which is why the explicit deny statement will yield more complete data for you.
* While you are creating an access list or after it is created, you might want to delete an entry. You can delete an entry from a named access list. Use the no permit or no deny command to delete the appropriate entry.
* In order to make the purpose of individual statements more scannable and easily understood at a glance, you can write a helpful remark before or after any statement by using the remark command.
* If you want to deny access to a particular host or network and find out if someone from that network or host is attempting to gain access, include the log keyword with the corresponding deny statement so that the packets denied from that source are logged for you.
* This hint applies to the placement of your access list. When trying to save resources, remember that an inbound access list applies the filter conditions before the routing table lookup. An outbound access list applies the filter conditions after the routing table lookup.

## **5.5 NAT (**Network Address Translation):

Network address translation is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

* Most computers on the stub domain communicate with each other using the inside local addresses.
* Some computers on the stub domain communicate a lot outside the network. These computers have inside global addresses, which means that they do not require translation.
* When a computer on the stub domain that has an inside local address wants to communicate outside the network, the packet goes to one of the NAT routers.
* The NAT router checks the routing table to see if it has an entry for the destination address. If it does, the NAT router then translates the packet and creates an entry for it in the address translation table. If the destination address is not in the routing table, the packet is dropped.
* Using an inside global address, the router sends the packet on to its destination.
* A computer on the public network sends a packet to the private network. The source address on the packet is an outside global address. The destination address is an inside global address.
* The NAT router looks at the address translation table and determines that the destination address is in there, mapped to a computer on the stub domain.
* The NAT router translates the inside global address of the packet to the inside local address, and sends it to the destination computer.

# Chapter 6- Results

## 6.1 Screenshots

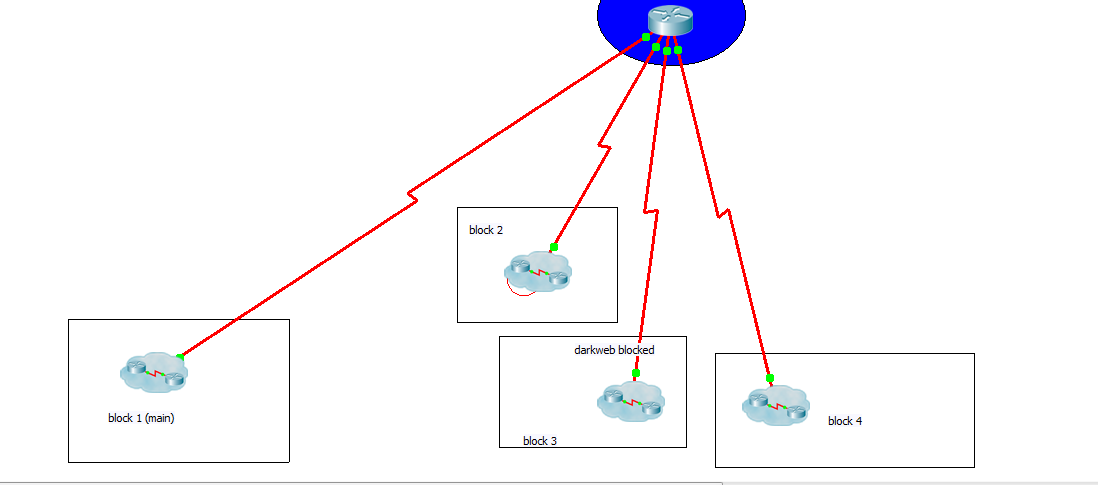
****

Figure :overall design

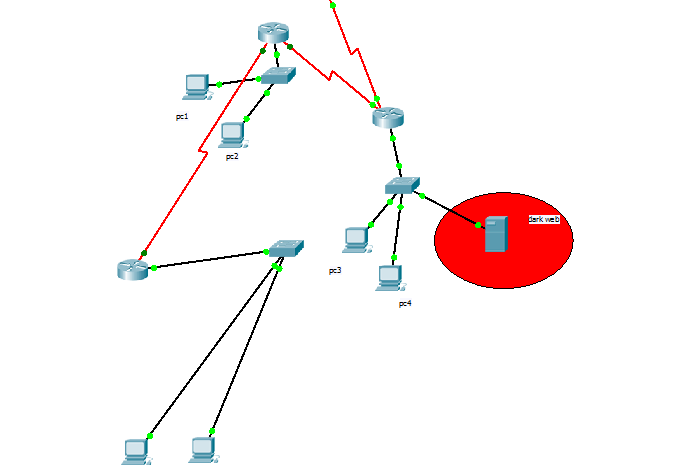


Figure : show the circuit and connection are completed

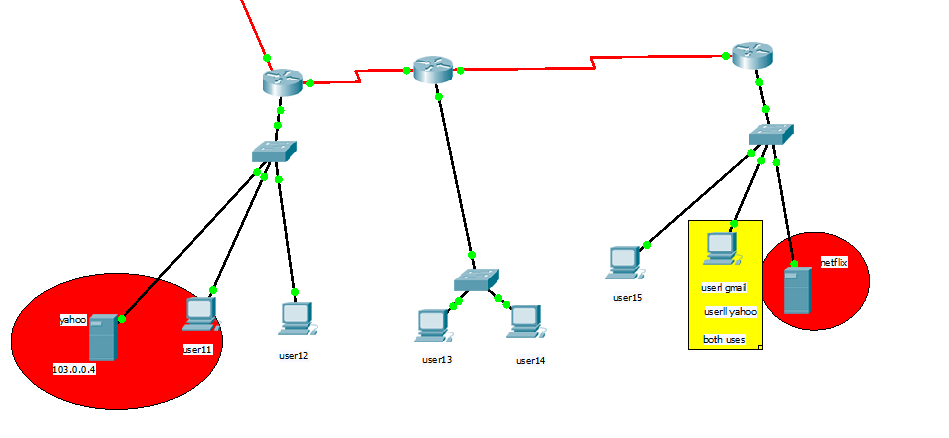


Figure :Different servers and routers

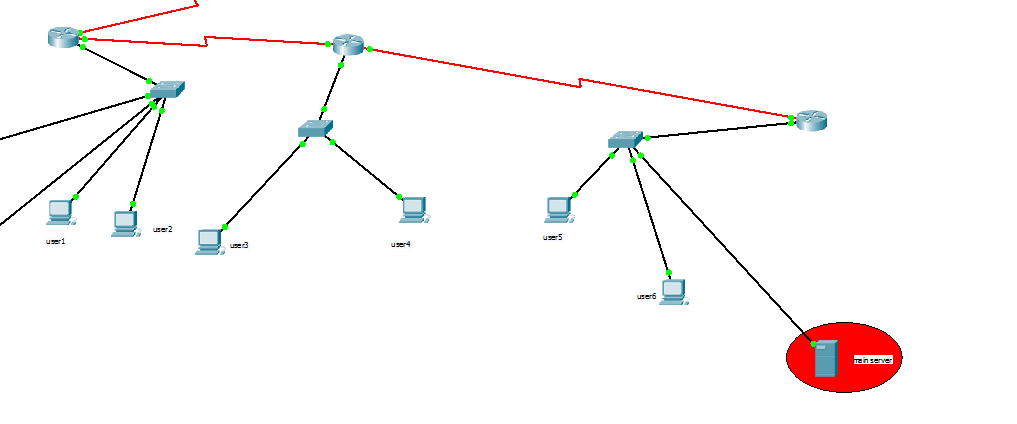


Figure :Main router- other blocks are connected with it.

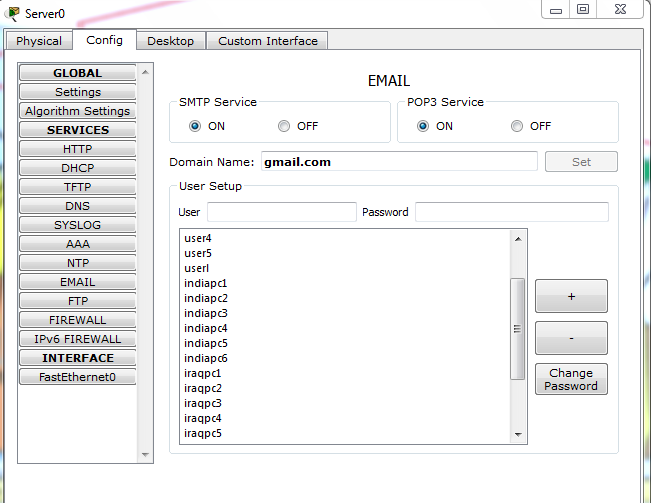


Figure :Username and password are added in database of Gmail

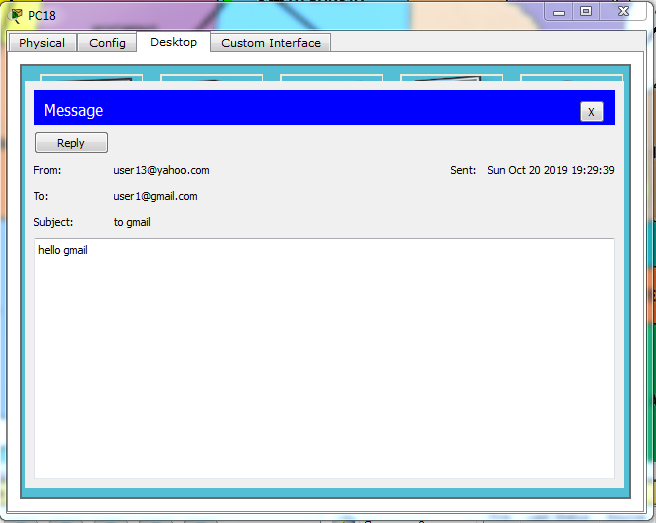


Figure :E-mail is received by user1 and we can reply back to him by click on reply button

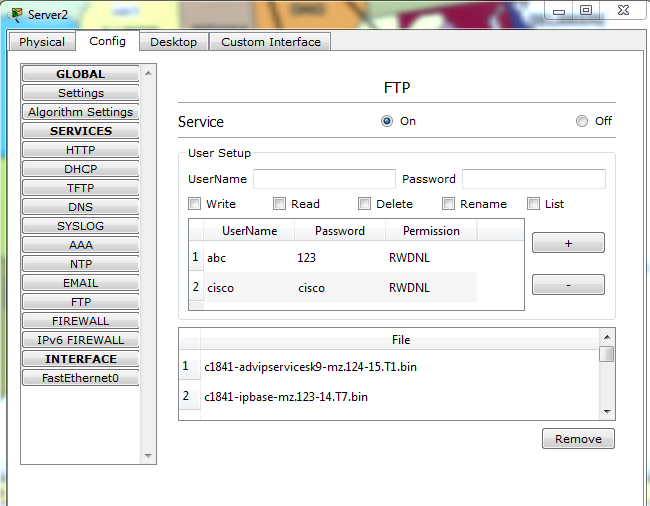


Figure : Service of file transfer protocol (FTP) is used

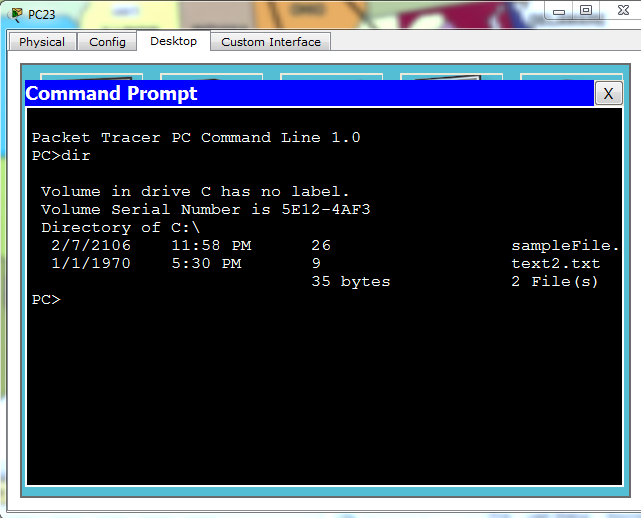


Figure :Protocol ftp is used and text is create and read by the user

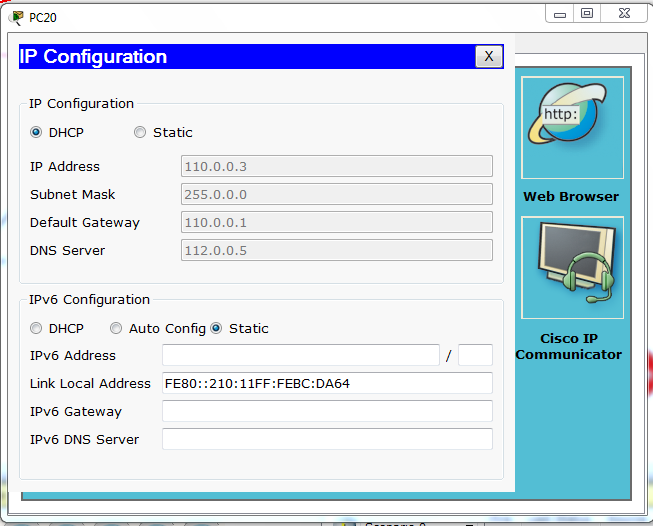


Figure :DHCP protocol

6.2 Output validation and Comparison:

* SMTP and POP3 are used to communicate with each other through emails.
* Username and password are used to send emails for security propose and we can change the password also.
* For the security, we configure the setting and reset the password.
* Access-list is used to block the unauthorized website on the web Brower.

# Chapter 7- Conclusion and Future scope

Network security is an important field that is getting more and more attention as the internet expands. The security threats and internet protocol should be analyzed to determine the necessary security technology. The security technology consists of mostly software based, as well as various hardware devices. In addition network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together. Securing the network is just as important as securing the computers and encrypting the message.

Points that must be considered when developing a secure network are:

1) Confidentiality: Information in the network remains private

2) Authentication: Ensure the users of the network are who they say they are

3) Integrity: Ensure the message has not been modified in transit

4) Authorization (access): providing authorized users to communicate to and from a

5) Non‐repudiation: Ensure the user does not refute that he used the network. An effective network security plan should be developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. Tools to reduce the vulnerability of the computer to the network include encryption, authentication mechanisms, intrusion‐detection, security management and firewalls.

# Chapter 8- References

* Ellis, J. and Speed, T. (2001) the Internet Security Guidebook, Academic Press.
* Anderson, R. (2001) Security Engineering: A Guide to Building

Dependable Distributed Systems, Wiley.

* [Behrouz A. Forouzan](https://dl.acm.org/author_page.cfm?id=81100279558)**, “**Cryptography and Network Security”, Vol. 1, 234-267, 1996.
* William Stallings**, “**Network and Internetwork security”, 134-146,1995.
* [Merike Kaeo](https://dl.acm.org/author_page.cfm?id=81371593199&coll=DL&dl=ACM&trk=0)**, “**Designing network security”, 34-56, 1999
* [Kenneth P. Weiss](https://patents.google.com/?inventor=Kenneth+P.+Weiss)**, “**Integrated Network Security System”, 279-326, 1991.
* Emis Stalling**, “**Cisco Network security”, 226-254, 1993.
* Andrew Forzam, “Wireless Network”, 87-115,1987.
* Standly Bros. “Security algos”, 156-201,1987.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***